## REMARKS

### I. Introduction

In response to the Office Action dated November 13, 2008, which was made final, and in conjunction with the Request for Continued Examination (RCE) submitted herewith, claims 1, 17, 30 and 46 have been amended. Claims 1-58 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

### II. Prior Art Rejections

In paragraph (2) of the Office Action, claims 1, 17, 21, 25, 30, 46, 50 and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dulude et al., U.S. Patent No. 6,310,966 (Dulude) in view of Krawetz, U.S. Publication No. 2003/0084301 (Krawetz). In paragraph (3) of the Office Action, claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53 and 55-58 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of Krawetz, and in view of Musgrave et al., U.S. Patent No. 6,202,151 (Musgrave).

Applicant's attorney respectfully traverses these rejections.

Applicant's claimed invention is patentable over the combination of references, because the claims contain limitations not taught by the combination. Specifically, Applicant's invention is designed to enable the authorized submission and authentication of biometric data and personal key in a confidential manner. In this regard, the biometric data and personal key are processed by an irreversible cryptographic algorithm causing the resulting data to be undecipherable, irreversible and undecryptable, but still capable of being used for comparison purposes. Moreover, all traces of the unprocessed biometric data and personal key are eliminated from the system and storage prior to any comparison.

The Office Action, on the other hand, asserts that the combination of Dulude and Krawetz describes all the limitations of Applicant's independent claims:

> As per claim 1, Dulude teaches:
>
> receiving a first biometric data and a first personal key; processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a fist processed data [Fig. 4, col. 6 lines 1-5, col. 5 lines 52-62]; receiving a second biometric data and a second personal key; processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm to form a second processed data [Fig. 5, col. 7 lines 7-14]; comparing the second processed data to the first processed data, without accessing the fist and second processed data in an unprocessed form in order to

enable authentication of first and second biometric data and personal keys in a confidential manner [Fig. 5, col. 7 lines 15-18]; and generating a signal pertaining to the comparison of the second processed data to the first processed data for use in an authentication process [Fig. 5, col. 7 lines 18-20].

Dulude teaches the authentication process without accessing the first and second processed data in an unprocessed form as above. Dulude doesn't expressively mention eliminating all storage or trace of unprocessed data prior to any comparison.

However, Krawetz teaches comparing the first processed data (verification signature) and the second processed data (check signature) for an authentication process [Fig. 3, paragraph 0023]. Further, Krawetz teaches eliminating all storage or trace of unprocessed data prior to any comparison [paragraph 0036 lines 10-15].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krawetz with Dulude, since one would have been motivated to protect the database of the server against susceptible to loss or theft of the data associated with a user [Krawetz, paragraph 0003, 0006].

Krawetz teaches the user data such as financial, personal or other type of sensitive or confidential information, and discarding or removing the unencrypted user data and identifier from the storage. However, Dulude teaches the user data includes the biometric data. Therefore, the combination of Dulude and Krawetz teaches eliminating all storage and trace of the biometric data and personal keys in an unprocessed form prior to any comparison.

As per claim 17, Dulude teaches:

receiving biometric data and personal key; processing the biometric data combined with the personal key through an irreversible cryptographic algorithm to form a processed data [Fig. 4, col. 6 lines 1-5, col. 5 lines 52-62]; comparing the processed data to a secondary data, without accessing the processed data in an unprocessed form in order to enable authentication of biometric data and personal key in a confidential manner [Fig. 5, col. 7 lines 15-18].

Dulude teaches the authentication process without accessing the processed data in an unprocessed form as above. Dulude doesn't expressively mention eliminating all storage or trace of unprocessed data prior to any comparison.

However, Krawetz teaches comparing the processed data (verification signature) and the second data (check signature) for an authentication process [Fig. 3, paragraph 0023]. Further, Krawetz teaches eliminating all storage or trace of unprocessed data prior to any comparison [paragraph 0036 lines 10-15].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krawetz with Dulude, since one would have been motivated to protect the database of the server against susceptible to loss or theft of the data associated with a user [Krawetz, paragraph 0003, 0006].

Krawetz teaches the user data such as financial, personal or other type of sensitive or confidential information, and discarding or removing the unencrypted user data and identifier from the storage. However, Dulude teaches the user data includes the biometric data.

Therefore, the combination of Dulude and Krawetz teaches eliminating all storage and trace of the biometric data and personal key in an unprocessed form prior to any comparison.

(Similar rejections are made for the other independent claims.)

These cited portions of Dulude and Krawetz are reproduced below:

Dulude: Fig. 4

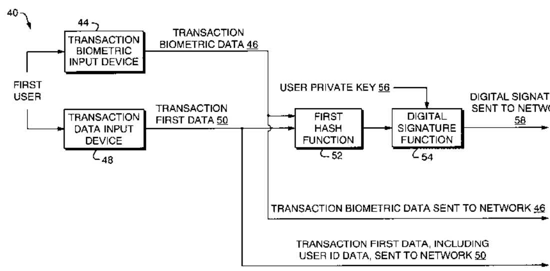



FIG. 4



Dulude: Fig. 5

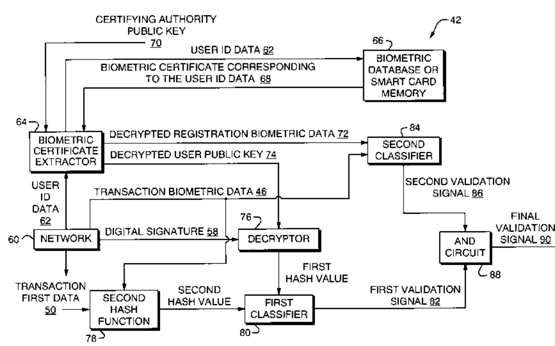



FIG. 5



Dulude: col. 5 line 50 - col. 6, line 12

Referring to FIGS. 4-5, to conduct an electronic transaction, the first user uses the transaction system 40 in FIG. 4. The first user uses a transaction biometric input device 44 to generate transaction biometric data 46 as contemporaneous biometrics associate with the first user. The first user also generates transaction first data 50 through a transaction data input device 48. For example, the transaction first data 50 may include selections of products to be purchased over the Internet, or may include electronic funds transfers through an ATM. The transaction first data 50 also includes user ID data identifying the first user and associating the first user with the remainder of the transaction first data.

Both of the transaction biometric data 46 and the transaction first data 50 are sent over the network 60 unchanged and in the clear, or optionally encrypted by additional encryption techniques known in the art, to be received by the transaction reception section 42, as shown in FIG. 5.

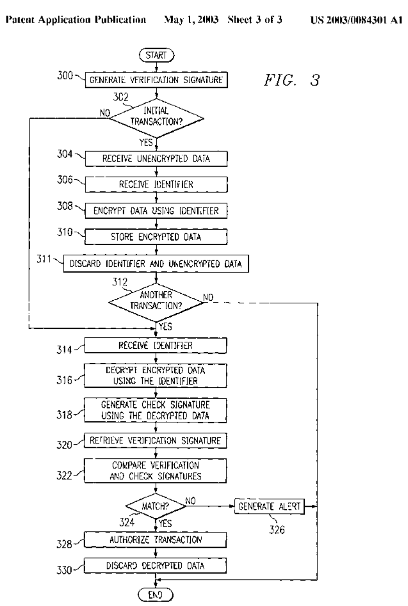
In addition, at the transaction transmission section 40 of FIG. 4, both of the transaction biometric data 46 and the transaction first data 50 are processed, for example, using a first hash function 52, such as a one-way hashing function, to generate a first hashed value. RSA and SHA-1 are examples of public key cryptographic methods and one-way hashing which may be used for such encryption and hashing functions. The RSA method is described, for example, in U.S. Pat. No. 4,405,829 to Rivest et al., which is incorporated herein by reference. The SHA-1 method is described, for example, in U.S. Pat. No. 5,623,545 to Childs et al., which is incorporated herein by reference.

Dulude: col. 7 lines 7-20

The receiving section 42 authenticates the first hash value by attempting to recreate the first hash value using a second hash function 78 which is identical to the first hash function 52 of the transmitting section 40. The second hash function 78 receives the transaction biometric data 46 and the transaction first data 50 from the network 60, which were sent from the transmitting section 40 in the clear, or optionally encrypted by additional encryption techniques known in the art. The second hash function 78 thus generates a second hash value from the same input data applied to the first hash function 52.

The first and second hash values are then compared by a first classifier 80, such as a comparator or matching routines in software, for determining a match between the first and second hash values. A first validation signal 82 is generated to indicate whether or not both independently generated hash values match.

Krawetz: Fig. 3



Krawetz: paragraph 0003

[0003] However, a PIN or other type of password offers limited security of the sensitive or confidential information stored on the server. For example, the database of the server remains susceptible to loss or theft. Additionally, users generally limit the length of a password or PIN to familiar dates or terms and to a quantity of digits that is easy to memorize and remember. Accordingly, passwords or PINs may be easy to crack or obtain, for example, by utilizing various iterative software programs.

Krawetz: paragraph 0006

[0006] In accordance with another embodiment of the present invention, a method for secure data transmission comprises receiving at a recipient device unencrypted data and an identifier on an initial transaction. The method also comprises encrypting the unencrypted data using the identifier to form encrypted data. The method also comprises discarding the unencrypted data and the identifier. The method further comprises decrypting at the recipient device the encrypted data in response to receipt of the identifier on a subsequent transaction.

Krawetz: paragraph 0023

[0023] To further authenticate and/or verify proper decryption of data 100, signature application 86 generates a check signature 110, which is stored in database 90, based on decrypted data 102. Check signature 110 is verified against a verification signature 112 stored in database 90. Verification signature 112 is generated based on data 52. For example, as briefly described above, server 20 may receive data 52 from client 18 to accommodate encryption and storage of data 52 as data 100. Signature application 86 may be used to generate verification signature 112 using data 52. Alternatively, verification signature 112 may also be retrieved from a remote storage area or device. Verification signature 112 may also be stored to server 20 by a network administrator, for example, in an ATM or bank card application. If signature 110 does not match signature 112, processor 80 may be configured to generate an alert or alarm to either a user or network administrator of system 10 indicating improper authentication or the unsuccessful attempt to access or use encrypted data 100.

Krawetz: paragraph 0036

[0036] At step 306, server 20 receives identifier 60 from client 18. In this example, the security level associated with identifier 60 is to be considered as having exceeded the minimum predetermined security requirements and, therefore, generation of padding data 62 and padded identifier 64 was not required; however, it should be understood that in the method illustrated in this FIG. 3, identifier 60 may be replaced with padded identifier 64 if security level requirements associated with identifier 60 required the generation of padding data 62 and padded identifier 64. At step 308, encryption application 88 encrypts data 52 using identifier 60 as an encryption key. At step 310, encrypted data 100 is stored in database 90. At step 311, the unencrypted data 52 and identifier 60 are discarded or removed from memory 82 such that only encrypted data 100 remains in memory 82.

Applicant's attorney disagrees with this analysis.

With regard to the Office Action's assertion that Dulude, as its contribution to the combination, teaches most of the limitations of Applicant's independent claims, Applicant's attorney respectfully disagrees.

The cited portions of Dulude describe how first biometric data and first transaction data are sent over a network (optionally in an encrypted form), and that a hash function may be performed prior to transmission to generate a first hash value that is also sent over the network. The cited portions of Dulude also describe how the first hash value is authenticated when received, by generating a second hash value from the first biometric data and first transaction data received over the network (optionally in an encrypted form), and then comparing the second hash value to the first hash value that was received over the network, in order to validate the first hash value.

However, nowhere do the cited portions of Dulude compare the first biometric data and first transaction data against second biometric data and second transaction data. Moreover, no such comparison is performed while both first and second biometric and transaction data are encrypted.

Instead, in Dulude, the first and second hash values are both generated from the same first biometric data and first transaction data, and merely serve to verify that the first biometric data and first transaction data were not altered during transmission.

In addition, the Office Action admits that Dulude does not mention eliminating all storage or trace of unprocessed data prior to any comparison. Nonetheless, the Office Action asserts that Krawetz teaches comparing the first processed data (verification signature) and the second processed data (check signature) for an authentication process, and that Krawetz teaches eliminating all storage or trace of unprocessed data prior to any comparison.

With regard to the Office Action's assertion that Krawetz, as its contribution to the combination, teaches these limitations of Applicant's independent claims, Applicant's attorney respectfully disagrees.

The cited portions of Krawetz describe a method of secure data transmission, wherein, initially, a verification signature is generated and stored. Then, in an initial transaction, unencrypted data and an identifier is received. The unencrypted data is encrypted using the identifier and the encrypted data is stored, with the unencrypted data being discarded. In subsequent transactions, the identifier is received and used to decrypt the encrypted data. A check signature is then generated using the decrypted data, and compared against the verification signature. If a match occurs, the transaction is authorized and the decrypted data is discarded; otherwise, an alert is generated.

In contrast to Applicant's invention, however, the check and verification signatures of Krawetz are not compared while in an encrypted form. Moreover, in Krawetz, the encrypted data that is decrypted and then used to generate the check signature is not discarded until after the comparison is made with the verification signature. Finally, the data in Krawetz from which the check signatures are generated is not irreversibly encrypted; instead, it may be decrypted as needed.

Thus, when combined, Dulude and Krawetz describe something different from Applicant's claimed invention of protecting the biometric data and personal key from being captured and revealed (a) while in transit; (b) while stored in a database; and (c) during the comparison. In this regard, Applicant's invention eliminates all storage and traces of the biometric data and personal key after they are irreversibly encrypted and before any comparisons are performed.

Further, Applicant's attorney submits that Dulude and Krawetz cannot be combined in the manner asserted by the Office Action. Any attempt to combine the Dulude and Krawetz references would render them operable and incapable of performing the tasks for which they were devised. Consequently, the Dulude and Krawetz references cannot be combined to teach Applicant's claimed invention.

Musgrave fails to overcome the deficiencies of Dulude and Krawetz. Recall that Musgrave was cited only against dependent claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53, and 55-58, and only for teaching the various limitations of these dependent claims, but not the independent claims.

Thus, Applicant's attorney submits that independent claims 1, 17, 30 and 46 are patentable over Dulude, Krawetz and Musgrave. Further, dependent claims 2-16, 18-29, 31-45 and 47-58 are submitted to be patentable over Dulude, Krawetz and Musgrave in the same manner, because they are dependent on independent claims 1, 17, 30 and 46, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-16, 18-29, 31-45 and 47-58 recite additional novel elements not shown by Dulude, Krawetz and Musgrave.

## III. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicant's undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: February 13, 2009

By: /George H. Gates/
Name: George H. Gates
Reg. No.: 33,500

GHG/

G&C 30571.302-US-U1